5 FAM 500 TELECOMMUNICATIONS

5 FAM 510 TELECOMMUNICATIONS POLICIES

5 FAM 511 SCOPE

(TL:IM-21; 12-30-95)

This chapter contains telecommunications policies and procedures for all users of the telecommunications systems identified and specific personnel where indicated.

5 FAM 512 AUTHORITIES

(TL:IM-21; 12-30-95)

This chapter is based on the following authorities:

(1) 41 CFR, Chapter 201-24; Sub-part 201-21.6; Subpart 201-21.603

(2) Section 1348, Title 31 U.S.C.;

(3) Pub. L. 96-465 (Foreign Service Act), Section 206(b) and 22 U.S.C. 2G51a;

(4) Pub. L. 99-399; Omnibus Diplomatic Security Act, Section 401(f);

(5) 5 CFR 735.205;

(6) E.O. 12472 and 12958; and

(7) National Security Decision Directive 211.

5 FAM 513 TELEPHONE SERVICES

(TL:IM-21; 12-30-95)

a. Classified information may not be discussed on Department telephones unless the telephones are secure telephones, e.g., STU III (cryptographically protected telephones).

b. The following communications over the system are prohibited:

(1) Using foul or profane (offensive) language;

(2) Impersonating another person;

(3) Making nuisance calls;

(4) Interfering with the service of others; or

(5) Using the circuits for unlawful purposes.

c. It is illegal to obtain, attempt to obtain, or assist another in obtaining telephone service by:

(1) Rearranging, tampering with, or making connections with any facilities of the government; and

(2) Using false credit devices to avoid paying, in whole or in part, established service charges.

d. Incidents that involve suspected waste, fraud, and abuse must be reported to the Office of the Inspector General.

5 FAM 513.1 Local Calls

(TL:IM-21; 12-30-95)

Telephone services are used for official business only. Official business calls may include emergency calls and other calls determined to be necessary in the interest of the Government. Examples of calls that may be considered necessary in the interest of the Government are:

(1) Calls to home or doctor if an employee is injured or becomes sick at work;

(2) An employee is required to work overtime without advance notice and calls within the local commuting area to advise family of the change in schedule or to make alternative transportation or child care arrangements;

(3) An employee makes a brief call to a non-long distance number to speak to a spouse or minor children or those responsible for the children;

(4) An employee makes brief calls to a non-long distance number that can be reached only during working hours, such as a local government agency, bank, or physician; and

(5) An employee makes brief calls to non-long distance numbers to arrange for emergency repairs to home or car.

5 FAM 513.2 Long Distance Calls in the Local Area

(TL:IM-21; 12-30-95)

a. Employees must use calling cards obtained from their long distance carrier of choice to make personal calls to locations outside the local call area. Not all calls made from Washington, DC to 301 and 703 area code numbers are local. The local telephone directories contain detailed information.

b. An employee who does not have a personal long distance calling card and is faced with a personal emergency may make a long distance call with the supervisor's permission. The employee must reimburse the department for the call.

5 FAM 513.3 Long Distance Calls

(TL:IM-21; 12-30-95)

a. Bureau review and certification are mandatory for all long distance telephone call records and bills. Questionable calls, i.e., those determined to be made for unofficial reasons must be paid for by the caller. Bureau management may take other action prescribed by 5 CFR 735.205.

b. Users of the telephone system must not routinely accept collect calls without prior written approval from the Digital Systems Programs Division (A/IM/SO/DO/DSP, Room 2921).

c. Calls to home while on official travel may not be billed to the Department.

d. All official calls home must be authorized on the travel authorization to be reimbursable.

5 FAM 513.4 Answering Machines

(TL:IM-21; 12-30-95)

a. Requests by bureaus for approval to install answering machines may be authorized only in those instances where Definity AUDIX or INTUITY voice mail is not available.

b. All answering machine or voice mail recordings must provide an alternate telephone number to call in emergency situations or for additional information.

5 FAM 513.5 Telephone Equipment

(TL:IM-21; 12-30-95)

a. The Digital Systems Programs Division (A/IM/SO/DO/DSP) authorizes all equipment or transmission facilities. Offices must receive permission in writing from the A/IM/SO/DO/DSP Division Chief to procure services or equipment not furnished by A/IM/SO/DO/DSP.

b. Employees must not install, disconnect, rearrange, remove, or attempt to repair equipment or facilities furnished by the Digital Systems Programs Division (A/IM/SO/DO/DSP).

c. Expenses incurred by damage, loss, theft, lost services, or destruction of any government-owned telecommunications equipment due to an employee's or other authorized person's negligence or willful act will be paid by the employee or other authorized user.

5 FAM 513.6 Posts Telephone Equipment

(TL:IM-21; 12-30-95)

a. Foreign Service posts operate post telephone systems and equipment and hire telephone operators locally. Posts also hire telephone technicians locally with specific authorization from RIMC and/or A/IM/SO/TO/MT/VO. Access to Controlled Assess Areas (CAAs) and Private Branch Exchange (PBX) equipment rooms at all posts by locally hired personnel is restricted. See provisions in the *Security Standards Handbook* published by DS.

b. The Regional Information Management Center (RIMC) must approve all post procurement orders for telephone equipment before they are submitted. All revisions or additions to overseas telephone systems, including those of AID or USIA, must be coordinated with the RIMC or A/IM/SO/TO/MT/VO for technical guidance. Neither RIMC nor A/IM/SO/TO/MT/VO will install or maintain AID- or USIA-purchased equipment if the Department has not been involved in the technical selection process and sanctioned the purchase.

c. Posts must submit all orders to A/IM/SO/TO/MT/VO for price quotes and ordering instructions.

d. All U.S. foreign missions are encouraged to use STU-III instruments in the secure mode to conduct routine business.

5 FAM 513.6-1 Controlled Access Areas (CAAs)

(TL:IM-21; 12-30-95)

a. In accordance with security standards for non-secure telephones (Security Standards published by DS), only Department-approved telephone systems and DS-approved instruments are approved for use in Controlled Access Areas (CAAs). Foreign manufactured telephone systems or instruments are not authorized for use in security sensitive areas.

b. Security requirements prohibit using speakerphones within the Controlled Access Areas (CAAs) at Foreign Service posts. See the Security Standards Handbook for more information.

c. Telephones used in CAAs must be secure and stored separately from telephones accessible to Foreign Service Nationals (FSNs). Telephones outside a CAA may not be introduced into a CAA unless they have been checked out by RIMC or other appropriately cleared technician as designated by A/IM/SO/TO.

d. Telephone Security Group (TSG) approved telephone instruments that have not been under continuous US control must be inspected by a Security Engineering Officer (SEO) before introduction into a CAA.

5 FAM 513.6-2 Cellular Telephones at Posts

(TL:IM-21; 12-30-95)

a. Cellular telephones may be used by post as an alternative to purchasing or leasing short range UHF and/or VHF administrative radio systems. Cellular telephones lack a broadcast feature that is required for security applications, which precludes their use for Emergency Action Plan purposes or nets. Cellular telephones do not meet diplomatic security requirements for transmissions at a classified level.

b. Cellular telephone instruments may not be used or stored in the stand-by state in a CAA without the approval of the Regional Security Officer (RSO) and post Counter-Intelligence Working Group (CIWG). The use of cellular phones in CAAs is restricted. See provisions in the *Security Standards Handbook* published by DS.

c. Cellular phones are not to be used as an alternative to regular phones in residences.

d. All cellular telephone purchases must be made with post or bureau funds.

e. Posts should consider the following when contemplating the cellular telephone option:

(1) Cost of equipment (purchase, lease, or rental);

(2) Cost of life cycle maintenance and support should be included in the initial purchase, lease, or rental agreement;

(3) Local availability of on demand maintenance and support;

(4) Cost of cellular phone service (usage fees—local and long distance);

(5) Adequacy of controls and accountability for official versus personal use; and

(6) Security standards that stipulate the types of telephone instruments that may be used in CAAs and preclude using cellular telephones.

5 FAM 513.7 Funding

(TL:IM-21; 12-30-95)

The following identifies how telephones are currently funded. Additional guidance will be developed by the Joint Bureau Planning Sessions held each year in cooperation with regional and functional bureaus. As this guidance is developed, it will be added to this section.

5 FAM 513.7-1 Regional Bureaus

(TL:IM-21; 12-30-95)

Regional Bureaus coordinate and approve all post telephone replacement and/or upgrade programs and allot funds as necessary to procure telephone equipment and services other than complete initial requirements.

5 FAM 513.7-2 Foreign Buildings Operations (FBO)

(TL:IM-21; 12-30-95)

FBO funds telephone systems for new capital construction of office buildings and certain other major rehabilitation projects requiring replacement of all major systems, which may include telephone systems.

5 FAM 513.7-3 Diplomatic Telecommunications Service-Program Office (A/DTS-PO)

(TL:IM-21; 12-30-95)

A/DTS-PO funds life cycle system replacements. It also funds installation contracts to replace failed or existing switches.

5 FAM 514 FACSIMILE (FAX) TRANSMISSION

(TL:IM-21; 12-30-95)

a. This section addresses using the Facsimile (FAX) as a method of transmission only. See 5 FAM 400 , Records Management, for information on maintaining faxed information as records.

b. FAX machines are used for official business only.

c. Personnel using FAX machines to transmit memorandums, letters, or other documents that originate within the Department or a Foreign Service post are responsible for:

(1) Obtaining clearances,

(2) Assuring that all appropriate offices receive copies of documents transmitted; and

(3) Providing copies of all official correspondence to the Office of Information Services, A/IM/IS/OIS, Room 1239, for inclusion in the Department's official records.

d. All personnel, supervisory personnel in particular, are responsible for ensuring that these policies and procedures are followed.

e. The following provides general guidelines for using the FAX:

(1) Only UNCLASSIFIED information may be transmitted on standard FAX machines. Classified information may be sent via FAX only on specifically approved TEMPEST devices used in conjunction with an approved encryption/decryption device.

(2) Personnel using FAX machines must follow current procedures on lines of authority and maintaining official records (see 5 FAM 400 , Records Management).

(3) Correspondence between the Department and Members of Congress is subject to guidance issued by the Bureau of Legislative Affairs. Responses to inquiries from members of Congress or their staffs may not be sent by FAX. The Inspector General has statutory authority to report directly to the Congress pursuant to the Inspector General Act of 1978, as amended.

(4) The Department has designed a facsimile transmission label, Form DS-1905, to be affixed to facsimile equipment. The label is available from the Office of Information Services, Records Management Branch (A/IM/IS/OIS/RA/RD).

f. Only secure TEMPEST facsimile certified to meet NACSIM 5100A standards and listed in the Information Systems Security Products and Services List may be used to transmit or receive classified documents or sensitive information. The secure FAX must be used in conjunction with an approved encryption/decryption device and must be installed in accordance with appropriate security criteria.

g. The operation of all Department secure facsimile machines, in the U.S. or abroad, must have the prior approval of the Executive Secretariat (S/S). The installation of any secure facsimile machines including all non-Department TEMPEST FAX systems at Foreign Service posts must have the approval of the Chief of Mission.

h. FAX machines (TEMPEST or non-TEMPEST) to be used within the CAA must be installed and maintained by cleared U.S. citizens only. Equipment previously installed in areas where there has been uncontrolled access by non-cleared individuals must be tested and inspected by A/IM/SO/TO/OTSS prior to installation in a CAA. Non TEMPEST FAX machines are not authorized to be installed in CAAs without Telephone Security Group (TSG) approved disconnects. Non-TEMPEST FAX machines intended for installation in controlled access areas must have either been procured in country following Bureau of Diplomatic Security approved random procurement guidelines, or transported to site by secure means by a cleared U.S. citizen or with a seal indicating it has not been tampered with

5 FAM 515 VOICE RADIO SYSTEMS

5 FAM 515.1 General Policies

(TL:IM-21; 12-30-95)

a. All radio networks and their use by U.S. government personnel in a foreign country (except those personnel under the command of a U.S. area Military Commander) are under the authority and direction of the Chief of Mission (COM) in accordance with 22 U.S.C. 3927.

b. Heads of agencies other than State must obtain COM approval before obligating funds to acquire new radio networks or to make major changes to existing networks. A major change is defined as altering an existing radio network in size or technical characteristics enough to require the host government to relicense, issue new frequencies, or to increase the traffic affecting network access by current users.

c. International law requires host country consent before installing and using a wireless transmitter. The COM or a designee will consult with the host government to obtain consent and where practicable, obtain specific frequencies from the host government to ensure interference-free radio use.

d. All agencies under the authority and direction of the COM must participate in post Emergency Action Plan networks unless the COM determines that an agency is not required to participate.

5 FAM 515.2 Radio Program Responsibilities

5 FAM 515.2-1 A/IM/RM/IAA

(TL:IM-21; 12-30-95)

A/IM/RM/IAA coordinates reciprocity issues for the foreign affairs community with M/OFM and with DS/DSS/OP when agreements involve emergency or security networks. A/IM/RM/IAA also prepares and coordinates interagency agreements relating to new radio networks and major changes to existing networks, and their use, as necessary.

5 FAM 515.2-2 Deputy Assistant Secretary for Information Management

(TL:IM-21; 12-30-95)

The Deputy Assistant Secretary for Information Management (A/IM) is the Accountable Property Officer (APO) for IM program property. The APO has delegated the duties of the Principle Custodian Officer (PCO) to the Chief of the Logistics Division, Office of Technical Operations (A/IM/SO/TO/LO). The Area Custodian Officer (ACO) is the post Information Management Officer (IMO) or Information Programs Officer (IPO). For details on APO, PCO, ACO, and IPO responsibilities, see 6 FAM .

5 FAM 515.2-3 IMO or IPO

(TL:IM-21; 12-30-95)

The IMO or IPO is the embassy's focal point for all radio matters. The IMO or IPO:

(1) Manages all Department HF, UHF and/or VHF radio systems and provides guidance to users of other radio systems under the authority and direction of the COM “as may be required to maintain Emergency Action Plan network discipline and operational efficiency, notwithstanding the ownership of these systems.” This includes consulting with host government authorities for operating licenses and frequency approvals;

(2) Provides radio operating procedures and maintenance guidance to radio equipment users;

(3) For systems funded by other agencies, assures that the agencies have provided all users and the IPO information and operator instructions to isolate and correct faults when an agency’s radio assets cause existing post or host country networks to degrade;

(4) Determines test schedules and procedures; and

(5) Is the area custodian of IM property.

5 FAM 515.2-4 Regional Security Officer (RSO)

(TL:IM-21; 12-30-95)

The Regional Security Officer (RSO) ensures that procedures used for transporting, storing, and using radio equipment within Department of State facilities comply with the Department’s Unclassified Electrical/Electronic Equipment security standards and Department policies.

5 FAM 515.2-5 A/IM/SO/TO/MT

(TL:IM-21; 12-30-95)

A/IM/SO/TO/MT is the Department program manager for voice radio systems (whether leased or government-owned), except for systems owned and operated by other agencies or provided to and operated by host governments.

5 FAM 515.2-6 Regional Information Management Center (RIMC)

(TL:IM-21; 12-30-95)

The Regional Information Management Center (RIMC) provides direct technical and operational support to each COM within its geographic area of responsibility. The RIMC reviews and approves post and contractor equipment specifications and technical plans to ensure compliance with the Department’s established radio program standards and specifications. For post or bureau funded systems, the RIMC assesses the probability of and

recommends resolutions to interference problems. It also provides technical assistance on integrating new systems or major changes in existing systems with other existing and planned radio systems. The RIMC provides similar advice to the COM with regard to other agency systems.

5 FAM 515.3 Reciprocity for Short Range Radio Systems

(TL:IM-21; 12-30-95)

U.S. law prohibits licensing foreign governments or their representatives to operate short range radio systems. Employees must not offer reciprocity in return for introducing and using short range UHF and/or VHF radio systems at overseas posts. Foreign governments may subscribe to commercially offered cellular radio services in the U.S. Foreign governments may also enter into commercial arrangements with U.S. firms licensed to provide, for example, security guard or motor pool services. These firms hold the necessary licenses and their U.S. employees operate the radios (including radios on Embassy or Consulate grounds).

5 FAM 515.4 Reciprocity for Long Range Radio Systems

(TL:IM-21; 12-30-95)

U.S. law permits a foreign mission, in special circumstances and on the basis of reciprocity, to construct and operate upon the recommendation of the Secretary of State and with the approval of the Secretary of Commerce, a fixed low-power transmitter in Washington, DC for communications to points outside the U.S. These installations must respect local zoning, land use planning, historical preservation, structural codes and similar building regulations. For information on obtaining host country consent, contact A/IM/RM/IAA.

5 FAM 515.5 Interagency Agreements

(TL:IM-21; 12-30-95)

The provisions of voice radio agreements currently in place at the Washington level remain in effect.

5 FAM 515.6 Funding

(TL:IM-21; 12-30-95)

a. Department funded systems may be owned or leased. IM funds Emergency Action Plan program radios. All other radio requirements are funded by the post or bureau. Additional guidance will be developed by the IM Executive Planning Sessions held each year in cooperation with regional and functional bureaus. As this guidance is developed, it will be added to this section.

b. Other Agency Funded Systems—Other agencies may own or lease radio systems at overseas posts subject to the conditions described in this chapter.

c. All proposals relating to introducing new radio systems or making major changes to existing systems must be coordinated with the COM or the designee and the Department (A/IM/RM/IAA).

5 FAM 515.6-1 Department (A/IM) Funded Systems

(TL:IM-21; 12-30-95)

a. A/IM funded Emergency Action Plan radio systems provide protection and security to United States Government personnel and property at overseas posts, including warden systems, convoy control and staging areas.

b. The RIMC or Department personnel provide life cycle support.

c. Equipment is provided based on Emergency Action Plans. A/IM provides radio equipment to all direct hire State Department personnel, Marine Security Guards, and the Heads of Section of other United States Government agencies represented at posts as required. Radio equipment for the remaining employees of other agencies is the responsibility of that agency.

d. The Department may provide UHF and/or VHF Digital Encryption System (DES) radios, subject to availability of funds, to selected posts based on the technical threat level assignment on the Department's Consolidated Threat List (CTL).

e. A/IM funded radio systems may be temporarily used to protect distinguished United States Government personnel who visit the mission or host government and the officials of other agencies.

5 FAM 515.6-2 Post or Bureau Funded Systems

(TL:IM-21; 12-30-95)

Radio systems for purposes such as paging, spousal support, and day-to-day administrative functions are either post or bureau funded. RIMC, RSO, and A/IM/SO/TO provide technical guidance and validation based on applicable Federal standards and life cycle support. Life cycle support for these systems is a post or bureau responsibility.

5 FAM 515.6-3 Other Agency Funded Systems

(TL:IM-21; 12-30-95)

a. Radio systems funded and operated by other agencies are the property of the funding agency. These agencies are responsible for installation, life cycle support, and equipment accountability. The installation and use of these systems, whether part of the Emergency Action Plan and security nets or separate, are subject to procedures and/or restrictions established by the COM.

b. Other agencies must coordinate radio requirements with the Department (A/IM/RM/IAA) and obtain COM approval.

5 FAM 516 NETWORK SYSTEMS

5 FAM 516.1 Diplomatic Telecommunications Service (DTS)

(TL:IM-21; 12-30-95)

The Diplomatic Telecommunications Service Program Office (DTS-PO) provides network connectivity from an agency's designated overseas location(s) to the corresponding designated foreign and/or U.S. location(s). This connectivity provides the necessary transmission path(s) and associated support for high and low speed data transfer, voice, facsimile, and other services as required.

5 FAM 516.1-1 Responsibilities

(TL:IM-21; 12-30-95)

a. The DTS-PO is responsible for the international DTS network from the Information Program Center to Beltsville Information Management Center (BIMC), where services are routed via dedicated circuitry either to the Department or to non-Department user agencies' Washington area headquarters.

b. DTS-PO establishes standards and system requirements for the DTS network, facilities and equipment, and user connections to the network.

c. Local Area Networks (LANs) and similar systems at posts are generally the responsibility of A/IM, Regional Bureaus, and other agency representatives at post.

5 FAM 516.1-2 Requests for DTS-PO Services

(TL:IM-21; 12-30-95)

a. Requests for DTS services must be submitted in writing (memorandum or letter) from the Headquarters Deputy Assistant Secretary level (or designee) to Chief, DTS-PO/REQ. DTS-PO will subsequently prepare Requirements Definitions through a standard interview process with the appropriate requesting agency officials.

b. Foreign affairs field representatives must submit requests for validation by their parent agency headquarters through their normal channels.

5 FAM 516.2 Electronic Mail (E-MAIL) Transmission

(TL:IM-21; 12-30-95)

a. This section addresses using Electronic Mail (E-Mail) as a method of transmission only. See 5 FAM 400 , Records Management, for information on maintaining E-Mail messages as records.

b. E-mail is for official use by authorized personnel.

c. Department employees have no reasonable expectation of privacy with respect to E-mail. System personnel may give to law enforcement officials any potential evidence of crime found on Department of State computers. The Department reserves the right to access all messages sent or received on its electronic mail systems. Systems managers, systems administrators, records managers, and security officials may monitor the system to ensure that all electronic mail transactions follow the proper procedures. Informal messaging privileges will be revoked from violators.

d. Unclassified messages transmitted via electronic mail must have an appropriate handling label at the beginning of the message.

e. Employees may use the Department's Foreign Affairs Information System (FAIS) or the Classified Information Handling System (CIHS) to convey unclassified and classified information to persons on the FAIS network.

f. Employees must properly classify and mark informal messages. Send classified messages only on secure systems such as FAIS and Principal Officer's Electronic Mail System (POEMS).

g. Employees must promptly delete or print out sensitive information sent or received by informal messaging from electronic mailboxes.

5 FAM 516.3 INTERNET Electronic Mail (E-MAIL)

5 FAM 516.3-1 General Policies

(TL:IM-21; 12-30-95)

a. Access to the INTERNET through the Department of State's facilities is for official and unclassified use by authorized personnel. The DOSNet should remain the network of choice for intra-Departmental unclassified communications.

b. Users are not authorized to load software onto a Department networked computer that permits INTERNET E-mail to transfer files.

c. The Department reserves the right to access all messages sent or received on its electronic mail systems. Systems managers, systems administrators, records managers, and security officials may monitor the system. Therefore, users must never consider the system private.

d. Individual encryption schemes are not permitted. All encryption must be installed and authorized by appropriate systems managers.

e. Executable files (programs) may not be downloaded to network systems and no attachments are authorized.

5 FAM 516.3-2 Responsibilities

(TL:IM-21; 12-30-95)

a. Bureaus must authorize and approve INTERNET use. Employees are not authorized to use the Department's DOSNet to INTERNET connection until they have completed the registration form and received the DOSNet and INTERNET E-mail User's Guide.

b. Electronic information products (i.e., publications) must be approved in advance by submitting Form DS-1837, Request for Approval of New Publication, to the Bureau of Public Affairs.

c. Bureaus should consult with A/IM/IS/OIS/RA/RD to develop appropriate procedures for handling INTERNET E-mail records.

d. Users must ensure that only unclassified, non-sensitive data is transmitted via the INTERNET. Employees may not use the INTERNET for strictly internal Departmental communications if other Departmental E-mail systems (i.e., FAIS, DOSNet, or OPENNet) are available.

e. Users must review and delete mail to prevent overloading the system.

f. INTERNET users must take every precaution to prevent transmitting viruses or other hazardous files to the Departments computers and computer networks. Routine virus checking is recommended.

5 FAM 516.3-3 INTERNET Prohibitions

(TL:IM-21; 12-30-95)

The following are prohibited in using the INTERNET system:

(1) Unlawful or malicious activities;

(2) Abusive or objectionable language;

(3) Misrepresenting oneself or the Department;

(4) Chain letters;

(5) Activities causing congestion or disruption of the local system or INTERNET;

(6) Fundraising activities;

(7) Advertising, conducting a personal business, soliciting clients or making sales; and

(8) Gambling.

5 FAM 517 TACTICAL SATELLITE (TACSAT) COMMUNICATIONS

(TL:IM-21; 12-30-95)

Electronic monitoring is generally prohibited in the Department. However, certain equipment, e.g. TACSAT, requires constant monitoring for its continued operations.

5 FAM 517.1 Types of TACSAT Communications

(TL:IM-21; 12-30-95)

The Department relies on two types of Tactical Satellite (TACSAT) communications: (1) in-flight secure communications from the Secretary and other principals and (2) emergency communications for approximately 255 posts around the world. These frequencies must be monitored by an operator at all times to hear requests for connections, critical calls in crisis situations, and calls from the Secretary while airborne. The operator must also be able to listen for technical problems with the transmission or conflicting simultaneous uses of the frequencies. A log is kept showing the time of receipt of each transmission requesting connection to another party. The content of the transmission is not recorded.

5 FAM 517.2 Notification Procedures

(TL:IM-21; 12-30-95)

In accordance with 41 CFR, the Deputy Secretary of State has approved continuous monitoring of TACSAT communications using the procedures described below:

(1) Posts with TACSAT handsets must put a notification on each handset alerting the user that TACSAT communications are monitored for technical reasons and that use of the handset constitutes prior consent to the monitoring; and

(2) Before boarding an airplane from which calls are monitored, Department personnel and guests of the Department must each be provided a written memorandum alerting them to the monitoring and informing them that use of the TACSAT handset constitutes prior consent to the monitoring.

5 FAM 518 SATELLITE TELEVISION DISH ANTENNAS

(TL:IM-21; 12-30-95)

a. Satellite television dish antennas may be acquired and installed at U.S. Diplomatic Missions, including residences.

b. The Post Contracting Officer must obtain written documentation that the following conditions for installing an antenna have been met:

(1) The installation is in conformance with applicable host country laws and regulations (e.g., licensing, zoning, safety codes, copyright, historical, preservation) and U.S. copyright laws (6 FAM) on video clubs, and cablecasting addressed U.S. copyright concerns;

(2) Consultations were held with appropriate host government officials to ensure that television reception will not cause interference to existing or planned host country communication services;

(3) Post has funds available for purchase, transport and installation of all such antennas and ancillary equipment (e.g., TV monitors, cabling, spare parts, maintenance);

(4) Where necessary, the local labor will be escorted by a cleared American (e.g. if antenna is installed on the roof of a controlled facility by a local contractor); and

(5) Post has Department approval for antenna installation provided the antenna and TV reception will not interfere with existing or planned post communication services. The antenna cannot be installed on the roof directly above the Information Program Center (IPC). A ten foot spherical zone of control must be maintained around the IPC.

c. The Post must also have the concurrence of the RSO and must ensure that proper security precautions outlined below are taken:

(1) Television equipment is permitted in the restricted access areas in rooms where classified information is not discussed or processed;

(2) Operational requirements that mandate that television equipment be located in areas where classified information is processed or discussed (inside the CAA) must be validated by the Counter-Intelligence Working Group (CIWG);

(3) Televisions inside the CAA must be unplugged from electrical power and the antenna cable must be disconnected when not in use;

(4) When televisions inside the CAA are in use, classified material may not be processed or discussed;

(5) The six-foot separation requirement from TEMPEST equipment is applicable for the television and all antenna cabling. This includes equipment in adjacent spaces;

(6) If the cabling for televisions located outside the CAA must transit the CAA, prior approval from DS is required;

(7) All equipment must be installed by Top Secret cleared U.S. personnel;

(8) Maintenance of equipment in the CAA must be performed by Top Secret cleared U.S. citizens or by local repairmen under continuous surveillance and escort by Top Secret cleared U.S. citizens with a one-to-two ratio;

(9) Malfunctioning equipment returned to a U.S. government approved facility for repair must be transported by secure means either under continuous control of Secret cleared U.S. citizens or by approved technical means and seal; and

(10) Equipment may be procured in-country following DS-approved random procurement procedures. Equipment not locally procured must be transported to site by secure means either under continuous control of Secret cleared U.S. citizens or by approved technical means and seal.

d. The Post must obtain Department approval for the location and installation of the antenna. Post must ensure that structural, architectural, electrical, and water penetration concerns are properly addressed by providing the following information directly to A/FBO and A/IM/SO/TO/PIF/FC:

(1) Drawings showing the planned antenna and monitor location, structural support, waterproofing details, routes of cable runs, etc;

(2) Calculations for the design of the structural support, including the design wind and seismic loading;

(3) Photos of the antenna location and surrounding area (follow proper security precautions where necessary); and

(4) Size, weight, model, performance requirements, and manufacturer's literature for the antenna.

5 FAM 519 TELECOMMUNICATIONS OUTAGES AND RECOVERY ACTIONS

(TL:IM-21; 12-30-95)

Department domestic organizations and overseas posts must address telecommunications outages and anticipated recovery actions in their electronic information processing continuity of operations plans or contingency plans. Telecommunications outages can have a significant effect on the effective accomplishment of the Department's mission.